Appl. No. : 09/712,398
Filed : November 14, 2000

REMARKS

Reconsideration and allowance of the above-referenced application are respectfully requested.

Initially, the indication that claims 18 and 20 would be allowable if rewritten into independent form is appreciatively noted. Both claims 18 and 20 have been so rewritten herein (including some changes to improve definiteness as part of the amendment), and should be allowable as per the indication of same.

The error in not providing the section headings in uppercase format is regretted. These titles have been amended herewith.

To the extent that this objection was directed to the language that was used within the actual headings, note that rule 77 makes the specific language optional, and that other heading names may be acceptable.

Claims 2-5 and 18 stand objected to due to informalities. In response, these informalities have been corrected.

Claims 3-5 and 9 stand rejected under 35 U.S.C. 112, second paragraph, as allegedly being indefinite. In response, these instances of indefiniteness have been corrected.

Claims 1-2, 6-7 and 15-17 stand rejected under 35 U.S.C. 102(e) as allegedly being unpatentable over Applebaum. This contention is respectfully traversed for reasons set forth herein. Claim 1 requires storing encrypted information associated with the computer program, obtaining personal information as part of the startup sequence for the computer program, and then reading and decrypting that encrypted information and comparing the personal information with the decrypted information.

The computer program is allowed to run normally only if the personal information agrees with the decrypted information.

Applebaum clearly does teach at paragraph 52, reading biometric information and comparing that to stored information. However, there is no teaching or suggestion that the stored information is encrypted as required by claim 1. Admittedly, Applebaum teaches encrypting certain information. However, different kind of information is ncrypted. The information which is encrypted in Applebaum is personal information about the user that will be sent over the network; not personal information about the user that will be compared with the biometric information obtained from the biometric interface device to validate running the program. Therefore, it is respectfully suggested that Applebaum teaches encrypting different information than that claimed. Applebaum does not encrypt the encrypted information and compare the personal information with said decrypted information, as required by claim 1. Claim 1 therefore is patentable thereover for this reason.

We note that the rejection states that Applebaum decrypts the information in paragraph 22. While Applebaum does decrypt information, it does not compare the personal information with the decrypted information and use that comparison to allow the computer program to run normally as required by claim 1. Again the rejection refers to Applebaum's claim 36 which does describe determining personal information and comparing that against stored identification information, but teaches nothing about decrypting the information as required by the claim.

As a totally separate reason for patentability, there is also no showing in Applebaum that the biometric information is read as part of the startup sequence for the

program. It appears that the biometric information is read and only prevents launching identity information about the user. However, there is no teaching or suggestion in Applebaum that personal information is obtained "as part of the startup sequence for said computer program..." as claimed.

Claim 1 should therefore be allowable along with the claims which depend therefrom.

Claim 6 specifically defines allowing the program to run only if the biometric reader is attached to the port. The rejection states that Applebaum teaches this in paragraph 48. However paragraph 48 simply talks about the peripheral interface and teaches nothing about the program only being allowed to run "if said biometric reader is attached to said port". Note that detecting whether the reader is attached to the port is very different then MERELY detecting if the biometric information is available. By detecting that the reader is attached to the port, in addition to requiring the biometric information itself, the system obtains some measure of protection against spoofing. Applebaum never teaches detecting if the reader is attached to the port as part of his analysis.

The argument above, about checking biometric information as part of the start of sequence, is even further bolstered by the argument in the rejection of claim 7. When rejecting claim 7, the rejection seems to tacitly accept the concept that the software can run prior to checking the user's identity. Claim 7 is even further allowable, as it defines occurs during startup, and again Applebaum teaches nothing about this operation during startup. In addition, however, Applebaum teaches nothing about allowing the program to run in only the limited exception mode at this time. Admittedly, Applebaum

prevents access to a specified function if the personal identification does not match. However, there is no teaching or suggestion of allowing running in only this limited exception mode, as claimed.

Claim 15 has been amended to emphasize that the user interface decrypts encrypted reference biometric information and should be allowable for similar reasons. Claim 16 should be allowable for similar reasons to those discussed above with respect to claim 6. Claim 16 even further emphasizes that detecting if the device is attached to the port is done separately from detecting if the biometric information is available.

Therefore, each of these claims should be allowable for this reason.

Claims 8-14, 19 and 21 stand rejected under 35 USC 102 as allegedly being anticipated by Brody. Admittedly, Brody teaches a system which personalizes the software. In the Brody system, the personalization is carried out from the publisher by incorporating personalization into the software installation stream, that is, into the installation program itself. The present system uses a very different tactic.

According to the present system, a determination is made as to whether the program is verified for installation (e.g., using a serial number or the like). Once the program is verified for installation, then a reference biometric is obtained. This means that any user can install the software, but then reference biometrics are obtained at the time of installation. User(s) who do not match those obtained reference biometrics cannot use the software.

Again, this is a different kind of system than that required by Brody. Brody requires that the software publisher provide personalized information as part of the software installation. The software publisher cannot simply publish generic software in

a box, since each copy of the software apparently needs to be personalized. In contrast, the system now defined by amended claim 8 allows the software to be generically published but personalized during installation. Anyone, not just the person for whom the software was personalized, can install the software. However, once installed, the software becomes matched with the reference biometric, and cannot be installed by someone other a user who matches the reference biometric. For these reasons, each of the claims should be allowable over Brody.

Claim 9 is even further allowable, as it requires determining if the specified license has already been used. This would appear to be unnecessary id Brody who personalizes each copy of the program. Similar arguments apply for claim 10. In rejecting claim 10, the Examiner points attention to paragraphs like paragraphs 10 and 15 which describe how the prior art has recorded a unique serial number. However, Brody teaches personalizing each copy of the software, and therefore effectively teaches away from using such a unique serial number. Admittedly, Brody teaches finding and generating a unique identifier, but teaches nothing about using this to install the software so that the user's biometric information can be obtained at the time that the software is installed.

Claim 19 was also rejected based on Brody. It is noted that Brody teaches using the personalization to determine whether the software can be installed, not whether it can be run after installation. Claim 19 has been amended to emphasize that the operations occur for an already installed program. This further distinguishes over the cited prior art.

Appl. No. : 09/712,398
Filed : N vember 14, 2000

The remaining rejections, based on combinations of the references, should each be overcome by the above, and it is respectfully suggested that each of these claims should be individually allowable on their own merits.

In view of the above amendments and remarks, therefore, all of the claims should be in condition for allowance. A formal notice to that effect is respectfully solicited.

Please charge any fees due in connection with this response to Deposit Account No. 50-1387.

Respectfully submitted,

Date: 12/5/03

Scott C. Harris
Reg. No. 32,030

Customer No. 23844
Scott C. Harris, Esq.
P.O. Box 927649
San Diego, CA 92192
Telephone: (619) 823-7778
Facsimile: (858) 678-5082